REMARKS

The Applicants appreciate the thorough examination of the present application that is reflected in the Office Action. Applicants also appreciate the statement that Claims 23-32, 63-72, and 103-112 would be allowable if rewritten in independent form including all of the recitations of the base claims and any intervening claims. To facilitate early allowance of the application, Applicants amended Claims 23, 25, 63, 65, 103, and 105 to independent form including the recitations of the base claims and all intervening claims. Accordingly, Applicants submit that Claims 23-32, 63-72, and 103-112 are now in condition for allowance.

Applicants also submit that the other pending claims are patentable for at least the reasons that will now be explained.

Claim Amendments

Many of the method claims have been amended to eliminate recitations of "step" and many of the computer program product claims have been amended to eliminate "means" language. Furthermore, Applicants have amended many of the claims to remove the recitations of "securely operably connecting" and replace them with "establishing a secure, operable connection". Accordingly, Applicants submit that the claim objections in the Office Action have been overcome.

Applicants File Herewith a Terminal Disclaimer to Overcome the Provisional Obviousness-Type Double Patenting Rejection of Claims 1-27, 41-67, 81-107, and 117-120:

Claims 1-19, 41-59, 81-99 have been provisionally rejected under a nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/764,844. Claims 1-27, 41-67, and 81-107 have been provisionally rejected under a nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/761,899. Claims 37-40, 77-80, and 117-120 have been provisionally rejected under a nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/764,844.

Applicants submit herewith a Terminal Disclaimer disclaiming additional term over the copending U.S. Application Serial No. 09/764,844 and U.S. Application Serial No. 09/761,899. Applicants' agreement to provide a Terminal Disclaimer is to expedite issuance of the present case and does not admit that the present invention is obvious in light of the copending U.S. Application Serial No. 09/764,844 or U.S. Application Serial No. 09/761,899. Accordingly, withdrawal of the obviousness-type double patenting rejection is respectfully requested.

Amended Independent Claims 1, 20, 41, 60, 81, and 100 Are Patentable over Bjorn in View of England

Claim 1 has been amended to include the recitations of Claims 19 and 21. Independent Claims 41 and 81 have been amended in an analogous way to Claim 1. Claims 19 and 21 have been canceled.

Claim 20 has been amended to independent form including the recitations of Claims 1 and 19 from which it previously depended. Independent Claims 60 and 100 have been amended in an analogous way to Claim 20.

Because Claim 1 now includes the recitations of Claim 21, and Claim 19 from which Claim 21 depended, its patentability over the rejections that were previously applied to Claim 21 will now be discussed. Claim 21 was rejected under 35 USC §103(a) over U.S. Patent No. 6,125,192 to Bjorn et al. (Bjorn) in view of U.S. Patent No. 6,330,670 to England et al. (England). Amended Claim 1 recites:

> 1. (Currently amended) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:
>
> computer-readable program code that is configured to operate a security core which provides security functions;
>
> computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

> computer-readable program code that is configured to securely perform a transaction using the secure integrated device;
>
> computer-readable program code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction; and
>
> computer-readable program code that is configured to mark the securely performed transaction as not secure if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction.

Accordingly, the system includes code that detects whether all components participating in a secure transaction remain operably connected to the secure integrated device during the secure transaction. The system also includes code that marks a transaction as not secure if one or more of the participating components fails to remain operably connected to the secure integrated device during the secure transaction.

The specification of the present application describes this code, in accordance with some embodiments of the present invention, as follows:

> In the preferred embodiments, components that authenticate themselves to the security core must remain physically attached thereto throughout an application function. Application-specific processing may be provided within each application processing subsystem to handle detachment of a component. For example, if camera module 130 is unplugged from the security core in the middle of taking a photo, the camera would have no way to transmit the photo (since it is preferably dependent on the security core for power, I/O, image storing, and so forth). If this module 130 is subsequently plugged in to a second (different) security core, that second security core would preferably stamp any pre-existing data in the camera as "unsecure" as the data traverses the second core (for example, on its way to the I/O bus of the second integrated device for purposes of storing captured images in persistent storage). (Alternatively, the second device may be adapted such that it will not accept any previously-created data.) Marking a data stream "unsecure" indicates the security core's inability to vouch for the authenticity and untampered state of I/O or application processor data.

(Specification, Page 21, line 18 - Page 22, line 11, emphasis added.)

Accordingly, the system may conclude that a transaction is not secure if a participating component becomes disconnected, and may treat data that is later received from that reconnected component as "unsecure".

The Office Action appears to concede that Bjorn does not disclose at least the recitations of Claim 1 that are underlined above. However, the Office Action cites to England in an attempt to provide the missing teaching.

Applicants note that the Court of Appeals for the Federal Circuit has affirmed that to support combining or modifying references in a § 103 rejection, evidence of a suggestion, teaching, or motivation to combine or modify must be *clear and particular*, and this requirement is not met by merely offering broad, conclusory statements about teachings of references. *In re Dembiczak*, 50 USPQ2.d 1614, 1617 (Fed. Cir. 1999). In an even more recent decision, the Court of Appeals for the Federal Circuit has stated that, to support combining or modifying references, there must be particular evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, *would have selected these components for combination in the manner claimed*. *In re Kotzab*, 55, USPQ2d 1313, 1317 (Fed. Cir. 2000).

The Office Action on Page 11 states that "England et al. teaches further comprising steps of: .. Detecting .... (col. 2, lines 60-67); and Marking ... (col. 11, line 54 through col. 12, line 8)." Applicants respectfully submit that the Office Action has not provided evidence of a suggestion, teaching, or motivation, much less, *clear and particular* evidence to combine or modify Bjorn to include the teaching of England to disclose the recitations of Claim 1.

However, for the sake of argument, even if Bjorn is combined with England, they still would not teach the "computer-readable program code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction", or "computer-readable program code that is configured to mark the securely performed transaction as not secure if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction" as recited in Claim 1.

The Office Action contends that "computer-readable program code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction" is taught by England at Col. 2, lines 60-67, which states the following:

> Secure boot of an operating system is usually a multi-stage process. A securely booted computer runs a trusted program at startup. The trusted program loads an initial layer of the operating system and checks its integrity (by using a code signature or by other means) before allowing it to run. This layer will in turn load and check the succeeding layers. This proceeds all the way to loading trusted (signed) device drivers, and finally the trusted application(s).

England describes an operating system that performs a secure boot in which a trusted program is run at startup. England does not describe that the operating system would detect whether all components participating in a securely performed transaction remain connected. Accordingly, Applicants suggest that England does not provide any teaching of "code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction".

The Office Action also contends that "computer-readable program code that is configured to mark the securely performed transaction as not secure if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction" is taught by England at Col. 11, line 54 through Col. 12, line 8, which states the following:

> The operating system checks the signature of a component before loading it (block 303). If the signature is valid (block 305), the component has not been compromised by someone attempting to circumvent the boot process and the process proceeds to check the level of trust assigned to the component (block 307). If the signature is not valid (or if there is no signature) but the component must be loaded (block 319), the operating system will not assume the identity of a DRMOS upon completion of the boot process as explained further below.
>
> A plug-and-play operating system provides an environment in which devices and their supporting software components can be added to the computer during normal operation rather than requiring all components be loaded during the boot process. If the device requires the loading of an untrusted component after the boot process completes, a plug-and-play DRMOS must then "renounce" its trusted identity and terminate any executing trusted applications (block 323) before loading the component. The determination that an untrusted component must be loaded can be based on a system configuration parameter or on instructions from the user of the computer.

Accordingly, England describes a plug-and-play operating system in which devices can be added to the computer outside of the boot process. However, it contains no teaching that the operating system would detect whether one or more of components participating in a secure transaction remains operably connected, and it contains no teaching that the operating system would mark a securely performed transaction as not secure if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction.

Consequently, Applicants respectively submit that the Office Action has not established a *prima facie* case of obviousness of amended Claim 1 over Bjorn in view of England. Accordingly, Applicants request withdrawal of the rejection of Claim 1.

Independent Claims 41 and 81 contain analogous recitations to Claim 1, and are respectfully submitted to be patentable over Bjorn in view of England for at least the reasons provided above for Claim 1.

Claim 20 has been amended to independent form including the recitations of Claims 1 and 19 from which it previously depended. Claim 20 was rejected under 35 USC §103(a) over Bjorn in view of England. Amended Claim 20 recites:

> 20. (Currently amended) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:
>
> computer-readable program code that is configured to operate a security core which provides security functions;
>
> computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;
>
> computer-readable program code that is configured to securely perform a transaction using the secure integrated device;

> computer-readable program code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction; and
>
> computer-readable program code that is configured to abort the securely performed transaction if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction.

Accordingly, the system includes code that detects whether all components participating in a secure transaction remain operably connected to the secure integrated device during the secure transaction. The system also includes code that aborts a secure transaction if one or more of the participating components fails to remain operably connected to the secure integrated device during the secure transaction.

As was explained above, Applicants submit that the Office Action has not provided evidence of a suggestion, teaching, or motivation, much less, *clear and particular* evidence to combine or modify Bjorn to include the teaching of England to disclose the recitations of Claim 20.

As was also explained above, Applicants submit that even if Bjorn is combined with England, the combination of Bjorn and England still does not teach "computer-readable program code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction."

Moreover, Applicants submit that neither Bjorn nor England teaches "computer-readable program code that is configured to abort the securely performed transaction if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction."

The Office Action contends on Page 11 that "aborting the securely performed transaction if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction" is taught by England at Col. 12, lines 9-12, which states the following:

> Assuming the signature is valid (block 305) and the component is trusted (block 309), it is loaded (block 311). The trustworthiness of a component can be decided using various criteria.

Accordingly, England describes that a signature block is used to determine if a loaded component is trusted. England does not describe that the operating system would detect whether one or more components participating in a secure transaction remain connected to a secure integrated device during the secure transaction, and it does not teach that a secure transaction is aborted if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction.

Consequently, Applicants respectively submit that the Office Action has not established a *prima facie* case of obviousness of amended Claim 20 over Bjorn in view of England. Accordingly, Applicants request withdrawal of the rejection of Claim 20.

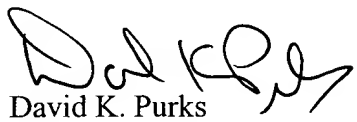
Independent Claims 60 and 100 contain analogous recitations to Claim 20, and are respectfully submitted to be patentable over Bjorn in view of England for at least the reasons provided above for Claim 20.

Dependent Claims 2-18, 22, 33-36, 42-58, 62, 73-76, 82-98, 102, and 113-116 are patentable per the independent claims from which they depend.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

Respectfully submitted,



David K. Purks
Registration No. 40,133
Attorney for Applicants and International Business Machines Corporation.

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401